AVOIDING AND RESOLVING DISPUTES OVER UNSATISFACTORY COMPONENTS

Kristal Snider and Daniel J. DiMase
ERAI, Inc.
Naples, FL, U.S.A.
ksnider@erai.com and dan@erai.com

ABSTRACT
Time and again, bad components get recycled into the electronics supply chain, inevitably leading to conflict between Buyers and Sellers. The best long-term solutions involve communication, investigation and mediation to avoid the need for litigation. This presentation will discuss the problem and how to converse openly relative to Buyer/Seller expectations, build a quality risk mitigation policy into your company's procurement and quality procedures, and how to go up the supply chain to ensure your suppliers and their suppliers are following best practices. Included will be an evaluation of vendor experience, vendor integrity, quality control, counterfeit avoidance & detection, testing requirements, contract terms and conditions, and data sharing.

Key words: communication, investigation, mediation and data-sharing.

INTRODUCTION TO THE PROBLEM
There has been a substantial increase in the number of reported counterfeit parts in recent years. Through the ERAI association, we have seen a tripling of reported counterfeit parts in 2007 compared to 2006 and a steady increase year over year since 2001 when we started monitoring the issue. [Appendix 1]

In addition, the U.S. Department of Commerce has reported that over 5% of global merchandise trade is counterfeit, costing the global economy over $650 billion dollars and costing the U.S. economy approximately $250 billion[1]. It also contributes to a loss of approximately 750,000 U.S. jobs. In 2006, over 5% of the total value of seized items from Customs and Border Patrol were consumer electronics. This figure increased to 9% in 2007[2].

The Government is concerned with counterfeit electronics affecting national security. There are potential issues with hidden backdoor codes being built into electronics that could potentially disrupt or change the original function of devices. Furthermore, they could provide access to sensitive information without the knowledge of the user. In September 2007, an article in IEEE Spectrum reported that Israeli jets avoided detection from a state-of-the art radar system in Syria. There was speculation that the microprocessors in the radar contained code that allowed the radar to be blocked[3]. There has been discussion and cause for concern that codes could be hidden in devices that could hypothetically turn our own missile systems against us.
There have also been reported instances of counterfeit networking gear being sold to government facilities such as the FBI, Navy, Air Force, Marine Corps, and the Federal Aviation Administration[4]. The consequence for undetected counterfeit network gear containing backdoor features for collecting sensitive data poses a serious threat to the integrity of these systems and to our nation's national security.

To add to the dilemma, Interpol has reported to the U.S. House Committee on International Relations that there are links between intellectual property (IP) crime to terrorist financing and organized crime syndicates. Interpol states that IP crime is one of the preferred methods of financing for terrorist groups[5]. IP crimes are typically considered a low-priority for law enforcement and provide a substantial return on investment for the counterfeiters with low penalties if they are caught and little to no jail time.

The Organization for Economic Co-operation and Development has identified additional effects of counterfeiting on multiple governments, including loss of tax revenues, additional expenditures to combat the problem, and corruption of government officials who are paid by the counterfeiters to overlook the issue[6].

The Government is not the only victim of counterfeit security issues. Corporate IT managers also need to be concerned with the security of their internal networks and must ensure that counterfeit network devices are not breaching their network integrity. Companies should also be concerned with potential backdoor entry when outsourcing their internal software systems.

There have been many documented cases of bribery and fraud at several organizations. Where there is money, there is corruption. Key decision makers have been bribed to look the other way for inadequate processes, to use known faulty or substandard material, or to perform an illegal activity such as selling rejected material out the backdoor of a manufacturer to the open market. Cases have been documented from lower level employees all the way up to senior management. In 2007, China executed the former head of its food and drug watchdog for approving untested medicine in exchange for cash[7].

U.S. companies lost approximately 5%, or approximately $652 billion[8], of annual revenues to fraud in 2006, according to Texas-based Association of Certified Fraud Examiners. Internal leaks are difficult to detect and require education and open communication within each organization to actively address the problem.

Counterfeit electronic parts can present a serious problem for the health and safety of consumers. In 2004, a 13-year-old boy was severely injured from an exploding counterfeit cell phone battery. There have been other reported instances of cell phones catching fire because of counterfeit batteries[9]. Electronic parts are used in a variety of applications from children's toys to critical medical equipment such as defibrillators and commercial airplanes. The potential liabilities incurred from counterfeit parts in these applications and others are cause for serious concern.

Original component manufacturers (OCM) have been inundated with phone calls of counterfeit failed material labeled with their brand. The OCMs have been dealing with loss of sales to illegitimate product, loss of reputation for failed material marked with their brand, and the cost associated with providing additional customer support and service for problems they did not generate.

Many of these component problems have led to expensive litigation. In 2007 John B Henry of eLawForum estimated the total annual cost of litigation for today's Fortune 500 companies to be $210 billion, equivalent to one-third of the after-tax profit[10]. This figure has likely increased since the time of this study.

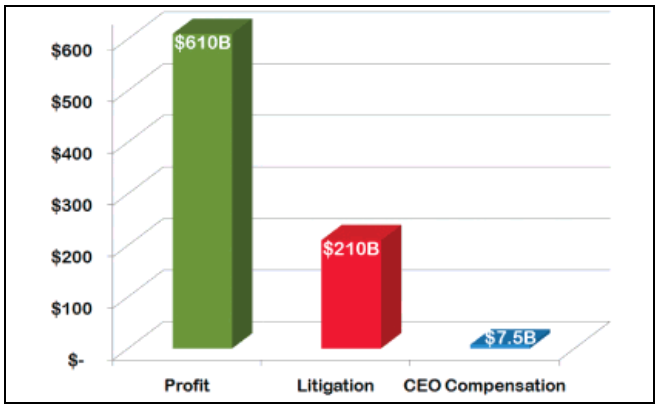


Figure 1. Comparison to Fortune 500 Profit (2006) (in billions)[11]

eLawForum reports the average "life" of a case extends to three years and purports this statistic applies to all areas of practice.

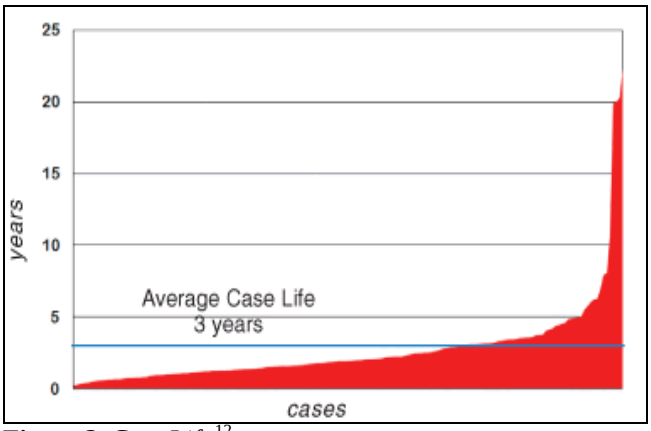


Figure 2. Case Life[12]

Corporations increase legal expenses by delaying case resolutions.

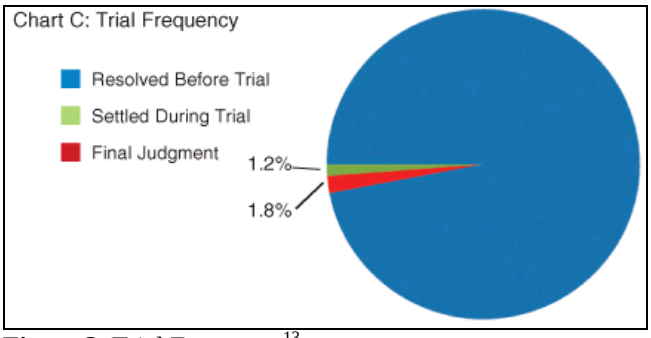


Figure 3. Trial Frequency[13]

eLawForum's study concluded only 3% of cases actually make it to trial.

CAUSES

Issues that have contributed to the counterfeit epidemic include the breakdown of global trade barriers, China and other emerging countries entering the World Trade Organization, and the explosion of the Internet that allows unscrupulous individuals to inexpensively advertise their fraudulent material to a worldwide marketplace.

Additional contributing issues to the counterfeiting problem can be attributed to misuse of the green initiatives such as the European Community's Waste Electrical and Electronic Equipment directive (WEEE) and the Reduction of Hazardous Substances directive (RoHS). Some companies have falsely claimed material is RoHS compliant or contains lead (pB) to adhere to the high-reliability marketplace. These situations are further forms of counterfeiting.

The green initiatives have also increased the need for recycling centers. Individuals think they are helping the earth when they drop off their used and broken electronic equipment to a recycling center. This would be true if the material was always being recycled responsibly. Unfortunately, some of these centers have been indirectly contributing to the counterfeiting problem. Some recyclers sell the working units immediately and give or sell the remaining scrap material overseas to the highest bidder.

Activists such as the Basel Action Network estimate that as much as 80% of the 400,000 tons of annual U.S. electronics waste, more often referred to as E-Waste, is shunted overseas to low wage nations such as China, India and parts of Africa due to mediocre or non-existent environmental standards and worker safety laws in these regions[14]. According to the U.S. Environmental Protection Agency, millions of tons of electronic waste is gathered and exported annually to these regions from all over the world. The electronics and precious metals are stripped in "dismantling shops", often in hazardous conditions, to maximize the return from the material. [Appendix 2]

This continuous supply of material is fueling the counterfeit market. It is well known that China is one of the largest recipients of e-waste and that they have found more than one way to profit from global waste disposal. In certain regions of China, entire communities rely on e-waste and counterfeit component trade as a source of revenue[15]. There are shops that are rumored to specialize in re-marking parts to resemble specific manufacturers in these regions.

When a counterfeit part is detected, the goods are often times returned to the Supplier in order for the recipient of the goods to obtain a refund. It is not uncommon for the counterfeit material to exchange hands numerous times before reaching its final destination. Evidence exists that proves known counterfeit items are re-circulated if they are not confiscated and disposed of appropriately.

Counterfeiting is a major issue that is clouding another serious problem in the supply chain that is not getting as much attention. As the electronics supply chain out-sources its manufacturing, the industry is facing problems in quality never experienced before as we become more dependent on the supply link directly above, with quality concerns outside of our typical process controls.

It is vitally important for procurement specialists to not only understand the scope of the problem but also modify their procurement strategies if they are to effectively lessen their exposure to counterfeits. This paper will provide readers with valuable trade principals that, if implemented and enforced, will aid your company in more safely navigating this sometimes unruly market.

RISK MITIGATION

Business people are supposed to make decisions based on economics. Unfortunately, procurement specialists sometimes take a "penny-wise, pound-foolish" approach when purchasing needed materials. The collateral consequences such as exorbitant legal costs, manufacturing interruptions, bad publicity, estranged customer relationships, and financial strains are the results of inadequate supplier verification, risk mitigation and counterfeit detection programs. Creating a trusted vendor program is essential, but without a rigorous counterfeit avoidance and detection program, it is not enough when maneuvering through today's complex global supply chain.

Research shows Buyers frequently deviate from their approved vendor programs. According to a survey conducted by Global Spec, 43% of survey respondents purchased material from distributors outside of their company's approved vendor list more than 10% of the time, and 26% said their company does not have an approved vendor list[16]. [Appendix 3]

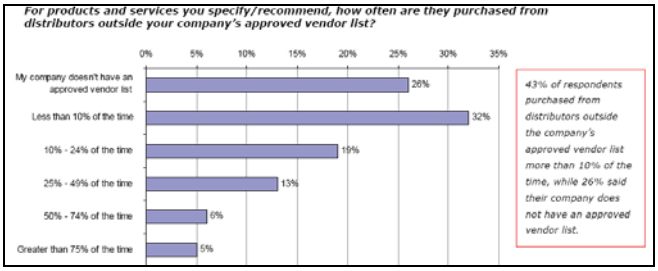


Figure 4.

When asked why they deviated from their approved vendor list, the majority of respondents stated it was because their approved supplier did not offer the product they needed[17]. [Appendix 4]

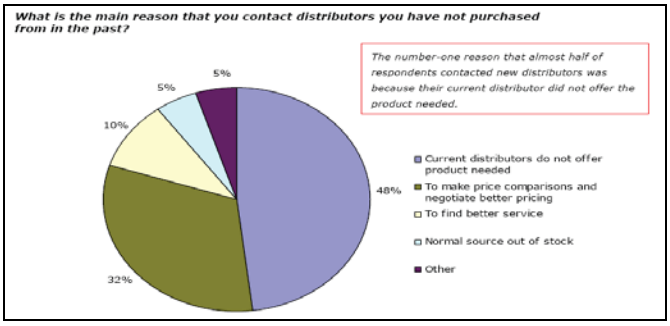


Figure 5.

89% of Global Spec's survey respondents have purchased parts online, with 37% reporting they purchase parts online at least once a week[18]. [Appendix 5]

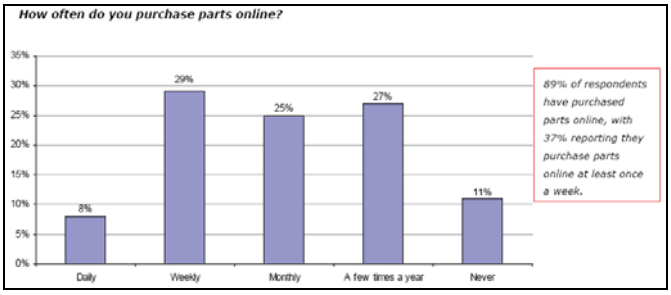


Figure 6.

SUPPLIER VERIFICATION

Understandably, competitive pricing, product availability and delivery are essential; however, procurement specialists should also evaluate vendor experience, vendor integrity, quality control, counterfeit avoidance and detection, testing

requirements, contract terms and conditions, and data sharing, and education. Each time one of these key-sourcing categories is bypassed, supply chain integrity is compromised.

Let's take a closer look at each of the above-mentioned categories.

Vendor Experience-

- The value of industry experience should not be underestimated. Veteran suppliers or those with several years experience have gained valuable industry insight and will be better equipped to avoid material originating from high risk areas and/or unscrupulous Sellers who are merely in search of a quick profit.

- Experienced suppliers can provide a verifiable trading history and will have knowledge dealing with known industry issues.

Vendor Integrity-

- Know with whom you are trading. How freely does the supplier divulge the identity and background of the corporate officers and senior management?

- Utilize industry resources to ensure the supplier does not have an unreliable or unsavory trading history. Has the vendor been reported to ERAI or GIDEP and do they have any unresolved past or pending complaints?

- A company's financial stability must be taken into consideration. Does the vendor have a favorable rating with D&B or other credit reporting bureaus? Can the supplier afford to support a product return should they supply nonconforming material?

Quality Control-

- Does the vendor adhere to the recognized industry terms and standards as outlined in your company's vendor agreement such as, but not limited to:
  - ISO 9001 – Quality Management Systems Requirements
  - AS-9100 – Quality Management Systems – Requirements for Aviation, Space and Defense Organizations
  - AS-9120 – Quality Management Systems – Aerospace Requirements for Stockist Distributors
  - EIA-481 Standard – tape and reel specification.
  - IPC/JEDEC-J-STD-003- Standard for handling, packing, shipping and use of moisture/reflow sensitive surface mount devices.
  - JEDEC standard No. 671 (JESD671) – Failure Analysis and Corrective Action.
  - JEDEC standard No. 625 (JESD625)- Requirements for handling electrostatic-discharge sensitive device
  - ANSI/ESD S20.20 – ESD Prevention Standard

(Please Note: Industry certifications do not guarantee that the company delivers products of superior (or even decent) quality. Emphasis should be placed on quality inspections and sourcing strategies.)

- Has the vendor implemented an industry recognized visual inspection standard such as the IDEA-STD-1010-A Acceptability of Electronic Components Distributed in the Open Market, or can they provide you with copy of their quality manual in which they define their inspection and counterfeit detection and avoidance practices?

- Can the vendor provide you with a copy of their vendor qualification protocol and a detailed explanation as to when, and if, they would deviate from following this guideline?

Counterfeit Avoidance and Detection-

- Has the vendor had special training in counterfeit detection?

- Has the vendor trained its key employees to ensure they are proficient in the implementation of corporate policies relative to vendor selection and counterfeit risk mitigation?

- Do you require the vendor to disclose in advance of the sale if the parts they are supplying have been procured from China or other known high risk trading markets?

- If your company policy is not to accept parts from known high risk trading markets, do you include language to this effect on your purchase order and do you require your vendor to also include the said language on their purchase order to their supplier to ensure supply chain integrity?

- Is it your company policy to require all products procured must have traceability to a known reliable source whenever possible?

- Does the vendor reference manufacturer datasheets to verify product package type and part dimensions?

- Does the vendor verify the authenticity of the product date and lot code directly with the OCM whenever possible and is it disclosed if this information is not available?

- Does the vendor utilize outside testing facilities to perform product authenticity verification, including, but not limited to, x-ray analysis, decapping and marking permanency, or can they perform these tests on site?

- Does your company have a policy for the confiscation and destruction of counterfeit material and is your vendor in agreement that known counterfeit devices should not be returned via the open market whenever possible?

- Does your vendor notify reporting agencies such as ERAI and/or GIDEP when counterfeit parts are identified?

Testing Requirements-

- Do you require your material to be tested?

- Does your vendor use independent testing facilities to conduct their visual inspections? If so, will they disclose the names of the lab(s) they will be using when verifying the authenticity and functionality of the goods they are selling to your company?

- If independent testing is conducted, is the testing facility certified to your standards?

- Do you require your vendor to notify you if they must deviate from the aforementioned list of approved test facilities to ensure the integrity of the third party inspections being performed?

- Is the test appropriate to adequately insure the authenticity and functionality of the device?

As stated by Kent Wade from Integra Technologies, "Maximum component assurance is achieved only through 100%, extended-temp, functional electrical testing to the OEM data sheet including burn-in and qualification testing."[19]

If the supplier thus far meets your vendor qualification expectations, continue the evaluation by engaging in an open dialogue relative to Buyer/Seller obligations. This can be accomplished by reviewing the terms and conditions that will be applied to all future trades.

Contract Terms and Conditions-

In addition to detailing product information, price, payment terms, and delivery expectations, a purchase order should also define how a Buyer and Seller would handle a nonconforming shipment. Buyers and Sellers should openly discuss their expectations and obligations. Failure to clearly define the terms of the agreement can result in costly contract disputes. These key points should be addressed:

- Goods: Buyer should clearly define the goods they seek to procure. In addition to including the manufacturer's part number also include date code, product package (i.e., BGA, PQFP, DIP, etc), packaging requirement (i.e., tube, tape & reel, trays, etc.), product condition (i.e., new, used, refurbished, etc.), quantity and manufacturer. Buyer and Seller should discuss if and under what circumstance a product substitute (i.e., cross) can and/or will be supplied or accepted.

- Buyer's Terms and Conditions Apply: Acknowledgment of the Purchase Order, shipment of any goods, or commencement of work pursuant to the Purchase Order may constitute an acceptance of the Buyer's purchase order contract. Often times, Buyers will include language in their agreement that stipulates no modification of or release from the Purchase Order will be binding unless agreed to in writing by both the Buyer and Seller. The parties should openly discuss any terms and conditions that are contradictory in order to avoid a "Battle of the Forms" scenario. Buyers will normally want their terms and conditions to supersede the Seller's terms. Will this be acceptable to your Vendor? Buyers and Sellers should work cohesively to ensure both party's interests are outlined and protected. Focusing solely on what is in the best interest of one party vs. the other increases your chances of a contract dispute should a quality problem emerge. Approach the purchase and sales agreements as a partnership. In doing so, both Buyers and Sellers will be fairly represented by the contract and the responsibilities of both Buyers and Sellers will be clearly defined. Escrow contracts can be used, not only as a form of payment, but to unify both the Buyer and Seller key terms and conditions, and to ensure that these conditions are met prior to funds being transferred.

- Product Identification and Traceability: If the product's lineage is a requirement, this should be divulged to the Seller. Buyers and Sellers should discuss the outcome and/or testing requirements should the product's lineage not be available and/or verifiable.

- Inspection: It is imperative Buyers and Sellers openly discuss the length of time it will take for the Buyer to conduct a proper inspection of the goods. What will be done during the inspection period? (i.e., visual inspection only or visual inspection and electrical testing?) Will the condition of the goods be altered during the inspection? Will the Buyer be required to pay for any parts destroyed during a destructive physical analysis or will the Seller absorb these costs? How long will the inspection period last? Does the Buyer reserve the right to reject goods based solely on visual nonconformities or will a formal test report be required? If the Buyer does not intend to immediately inspect and/or test the goods, but instead intends to place the material in stock for an unspecified period of time pending use, will the Seller honor a return authorization if a nonconformance is identified several months after receipt of the goods? If the Buyer is not willing or able to conduct the necessary inspection and/or testing during the agreed upon period of time, are they willing to sign a waiver which could limit the liability of the Seller?

- Rejection: If the goods are rejected, who will pay the return freight? If outside services such as an escrow provider were used to facilitate the transaction, will the Buyer be entitled to reimbursement for these fees? How will the goods be returned? Will the Seller be given the opportunity to replace the nonconforming goods? If not, what is the Seller's refund policy - cash or credit?

- Warranties: Buyers will rightfully expect Sellers to supply goods that are free from defects in materials and workmanship and in full conformity with Buyer's specifications, product drawings, and data sheets. However, Buyers and Sellers should openly discuss the Buyer's procurement history and usage, to ensure product failures and return requests are not the result of inappropriate use or failure due to application and/or handling.

- Confiscation and Destruction of Counterfeit Material: Is it the Buyer's policy to confiscate and destroy counterfeit material? If so, what evidence should Buyers produce to substantiate their claim the goods are indeed counterfeit? Clear protocol needs to be established prior to counterfeit confiscation and/or destruction. Counterclaims need to be addressed and answered prior to the destruction of suspect material. Will the confiscation and destruction of these goods prohibit the Seller from obtaining a refund from their supplier? How will the Buyer and Seller handle a transaction involving counterfeit material? Buyers and Sellers should openly converse about counterfeit product and how it would negatively impact the financial bottom line and relationship should there be an unforeseen occurrence.

- Remedies: The purpose of a remedies clause is to ensure that the parties' rights specifically provided for in the contract are in addition to their rights provided by the general laws of the presiding jurisdiction. For example, in a contract for the sale of electronic components, the Buyer may be entitled to require the Seller to make good or replace defective items, or perhaps the Buyer reserves the right to seek reimbursement for compensatory damages should the Seller provide nonconforming material. If the Buyer is going to require the Seller to carry the burden of losses exceeding the cost of goods or replacement cost of goods, this should be disclosed and discussed.

Data Sharing

- Companies should check databases such as ERAI and GIDEP for known high-risk parts, financially strained companies, and unreliable suppliers, enabling them to make more informed business decisions. Participation in these organizations does not guarantee quality but should help participating companies mitigate known industry problems.

- Companies need to proactively check part numbers on their assemblies and bill of materials against reported faulty and counterfeit items.

- Companies should assign a representative to report nonconforming parts to ERAI and/or the Government Industry Data Exchange Program (GIDEP) so that problems will not repeat over time for the reporting company when they have to procure the item again, for their subcontractors and various divisions, and for the benefit of other organizations.

- Companies should attend industry trade shows, conferences, and trainings ensuring they are in tune with the changing market and industry expectations.

- When a problem does arise, and they will despite your best efforts, it is imperative that Buyers and Sellers share their experience so others are warned. The complex issues facing the electronic supply chain require a united response. Service providers like ERAI and GIDEP provide businesses with a platform by which valuable data can be exchanged for the wellbeing of the overall industry.

DISPUTE RESOLUTION

Dispute resolution should be viewed as "assisted negotiation". A good dispute moderator will listen to all parties in the dispute, gather information, promote communication, advance understanding, and work to ensure a fair resolution ensues. Many supply chain disputes are the result of cancelled orders, unauthorized or unexpected material price adjustments, or the purchase and sale of nonconforming and/or counterfeit material. Because there is no guarantee dispute resolution negotiations will deliver positive results, it is always best if Buyers and Sellers take the appropriate measures to steer clear of conflict. Most disputes can be avoided if Buyers and Sellers clearly communicate their needs and expectations in advance of entering into contractual agreements. If the Buyer or Seller is considering dispute resolution as a means to resolve the conflict, select a moderator who abides by dispute resolution principals.

- Buyers and Sellers should discuss and agree in advance of initiating trades that if a dispute does arise both parties will enter into mediation in an effort to avoid litigation.

- Dispute resolution negotiations are voluntary. Buyers and Sellers should agree and be aware they can walk away from discussions at any time for any reason, while understanding that doing so could lead to litigation.

- Dispute resolution should be a collaborative effort. The moderator should encourage Buyers and Sellers to work together to solve problems and to reach what Buyers and Sellers perceive to be an evenhanded agreement.

- The moderator should use the original terms and conditions as a means to facilitate a resolution.

- Nothing should be imposed on the Buyer or Seller. Each party to the dispute can agree to accept or decline an offer if it is believed the offer in question is not in their company's best interest.

- Buyers and Sellers should verify, prior to entering into dispute resolution proceedings, that the mediation discussions and all materials developed for the mediation are not admissible in any subsequent court or other contested proceeding, except in situations when a finalized and signed Dispute Resolution Agreement has been entered into.

- The moderator has a responsibility to assist each mediating party and cannot favor the interests of one party over another, nor should the moderator favor a particular result in the dispute resolution process. The moderator's role is to ensure that Buyers and Sellers reach agreements in a voluntarily and informed manner, and not as a result of coercion or intimidation.

- No moderator can effectively perform if the individuals participating in the dispute resolution process do not have the authority to settle on behalf of their respective company.

- The dispute resolution process requires all parties participating in the effort do so in good faith by being willing to be flexible and sincere in their desire to resolve the conflict.

- Divulge your position to your moderator. It is best if both the Buyer and Seller provide the moderator with a summary which includes the facts of the case from their perspective, as well as a list of resolutions that would be acceptable prior to the mediation. This ensures the moderator can quickly focus on what is essential to bringing about a resolution.

- Be honest. Buyers and Sellers who misrepresent facts during the dispute resolution process empower the other party involved in the dispute. Mistruths imply there are significant weaknesses in a case.

- Listen with an open mind. Buyers and Sellers must be prepared to hear and understand the arguments being raised by the opposing party. An effective moderator will transfer information from the Buyer to Seller in a way that is truthful and direct but not offensive. The "good listener rule" especially applies to the moderator, who should be prepared to allow time for both the Buyer and Seller to "vent".

- Remember the risks. Both Buyers and Sellers should never forget failure to successfully negotiate a dispute resolution agreement could result in costly litigation. It is possible that neither the Buyer nor Seller may be completely satisfied at the conclusion of a dispute negotiation. Each party should be prepared to walk away equally dissatisfied.

Implementing the above-recommended strategies will safeguard a business from unnecessary financial losses. If a problem does arise, expensive litigations should only be used as a last resort.

CONCLUSION

Companies need to be aware of the potential hazards and their causes in today's supply chain. Current procurement and quality procedures cannot completely eliminate the potential of faulty parts making their way into your organization, inevitably leading to conflict between Buyers and Sellers. The best long-term solutions involve communication, investigation, and mediation to avoid the need for litigation.

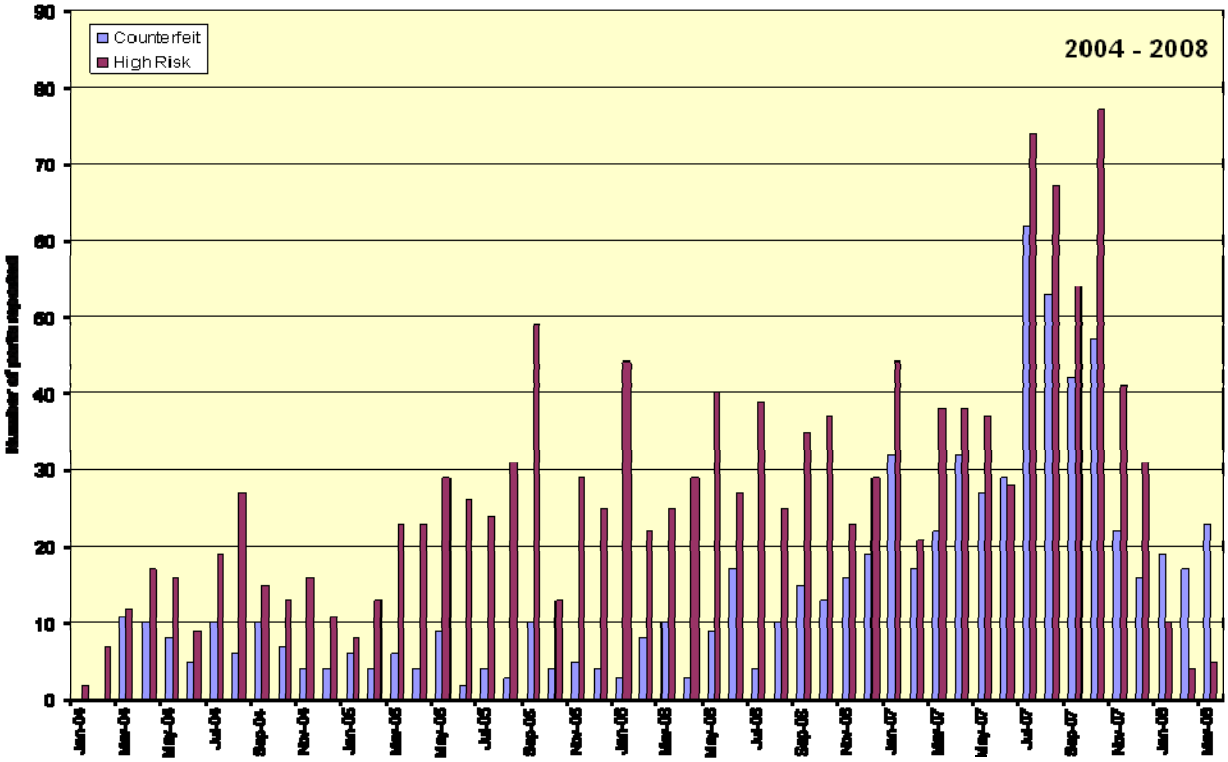
Organizations should be proactive in addressing potential problems before they occur. Risk mitigation strategies should be reviewed to address problems like counterfeiting that are plaguing the electronics marketplace. Quality control plans should be developed to address the risk and to ensure that the links up the supply chain ladder that support your business are following best practices. Due diligence should be performed in supplier verification.

REFERENCES

[1] US Chamber of Commerce, Global Intellectual Property Center, "Get the Facts", The True Costs.
[2] Ed Sperling, "The Battle Over Counterfeit Goods", Electronic Business, October 2007.
[3] Sally Adee, "The Hunt for the Kill Switch", IEEE Spectrum, May 2008 -
[4] Bob Brewin, "FBI Partially Lames Procurement Rules for Fake IT Products", Nextgov, May 2008.
[5] Ronald K. Noble, "The links between intellectual property crime and terrorist financing", Text of public testimony before the United States House Committee on International Relations, July 16, 2003.
[6] Organisation For Economic Co-operation and Development, "The Economic Impact of Counterfeiting and Piracy", 2007.
[7] CBS News, "China Executes Ex-Food & Drug Watchdog", July 10, 2007
[8] Eric Krell, "The Awakening", Business Finance, 2007.
[9] Associated Press, "Exploding Cell Phones", November 24, 2004.
[10] John B. Henry, "Fortune 500: The Total Cost Of Litigation Estimated At One-Third Profits", eLawForum.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Basel Action Network and Silicon Valley Toxics Coalition, "Exporting Harm – The High –Tech Trashing of Asia", 2002.

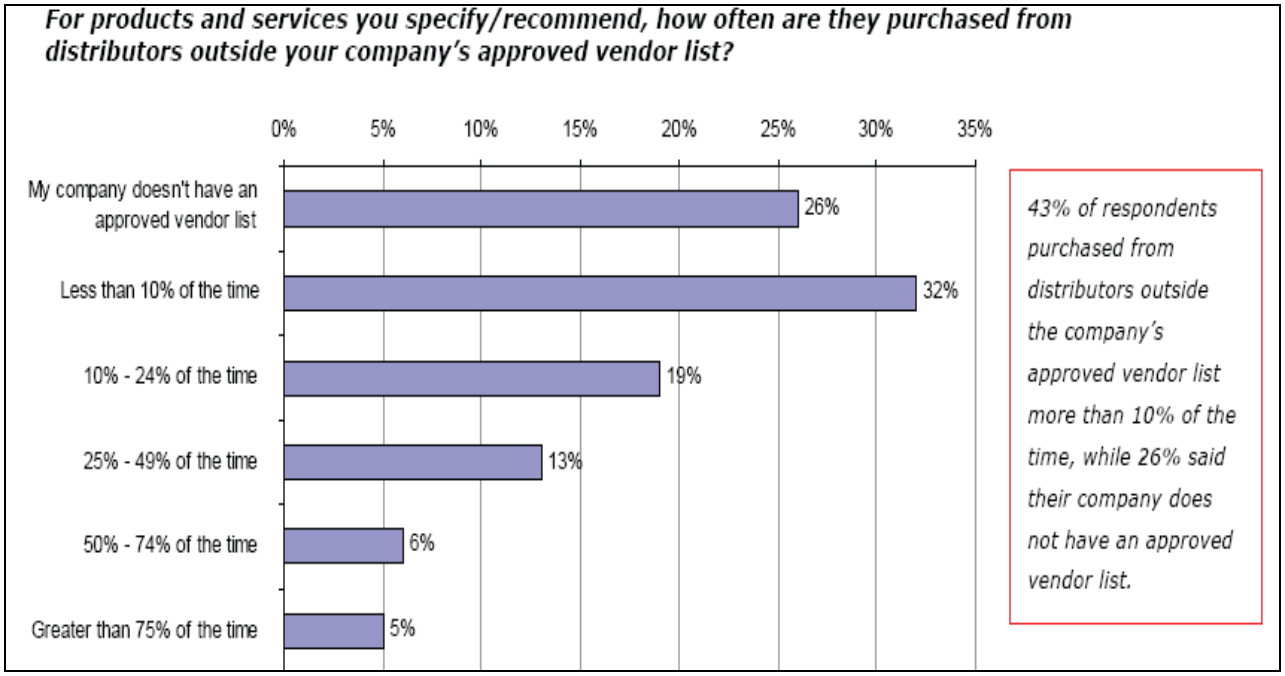
[15] Zhan Lisheng, “Local gov’t cleans up e-waste sector”, News Guangdong, August 24, 2005.
[16] GlobalSpec, “Distributor Buying Trends Survey of Electrical/Electronics Technical Professionals”, 2007.
[17] Ibid.
[18] Ibid.
[19] Kent Wade, “Counterfeit Semiconductors - Detection PlanVerify Semiconductor Manufacturer Authenticity”.

[Appendix 1]

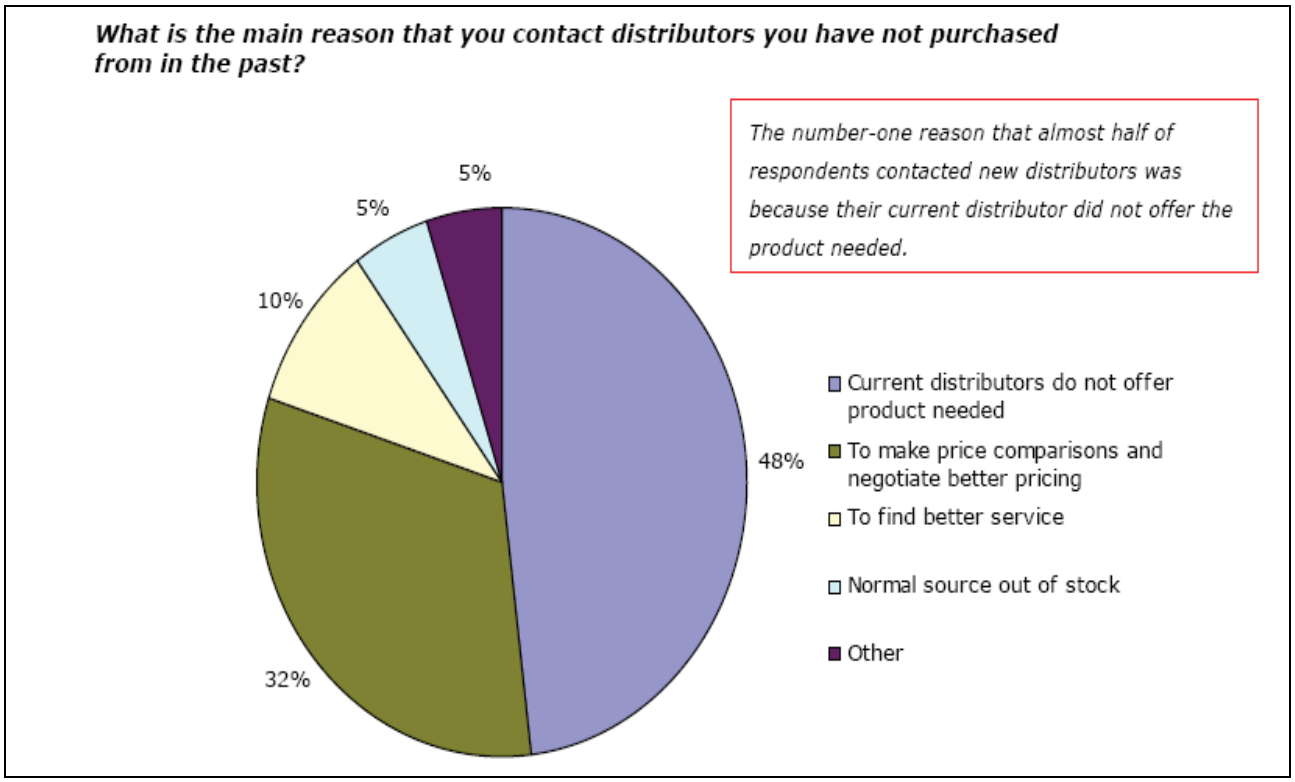


[Appendix 2]

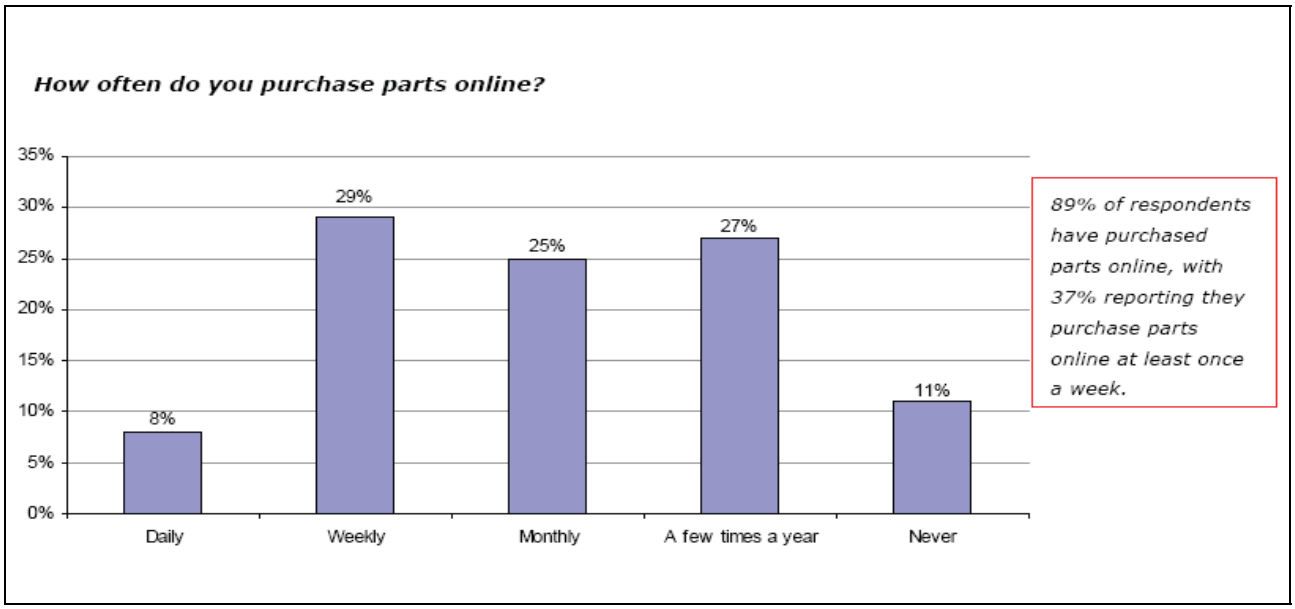
[Appendix 3]



[Appendix 4]



[Appendix 5]


How often do you purchase parts online?
35%
30%
25%
20%
15%
10%
5%
0%
8%
29%
25%
27%
11%
Daily
Weekly
Monthly
A few times a year
Never
89% of respondents have purchased parts online, with 37% reporting they purchase parts online at least once a week.